REGULATORY OBSERVATION

REGULATOR TO COMPLETE

RO unique no.:	RO-ABWR-0010
Date sent:	5th June 2014
Acknowledgement required by:	26th June 2014
Agreement of Resolution Plan Required by:	4th July 2014
Resolution of Regulatory Observation required by:	*To be determined by the Hitachi-GE Resolution Plan*
TRIM Ref.:	2014/138766
Related RQ / RO No. and TRIM Ref. (if any)**:**	
Observation title:	Design Basis Analysis of essential services and support systems
Technical area(s) Fault Studies	**Related technical area(s)** Electrical, PSA, Mechanical, C&I

Regulatory Observation

Summary

It is ONR's experience that "traditional" lists of design basis initiating events do not always explicitly include faults in essential services or support systems. ONR requires Hitachi-GE to demonstrate that it has comprehensive design basis analyses of all initiating events occurring in UK ABWR systems such as heating, ventilation and air conditioning (HVAC) systems, cooling chain systems and compressed gas systems. Partial failure of a system (e.g. failure of a single component or train) and total failure of a system due to a common cause failure (CCF) should be considered.

Background

The expectations ONR inspectors apply to the assessment of safety cases for nuclear facilities are set out in the HSE Safety Assessment Principles (SAPs). SAP FA.2 requires fault analysis to identify initiating events in a systematic, auditable and comprehensive manner. SAP FA.5 requires the safety case to consider the SAP FA.2 list of events and identify those which should be analysed with design basis methodologies.

It is ONR's experience that "traditional" lists of design basis initiating events do not always explicitly include faults in essential services or support systems. In many cases, they are implicitly bounded by other initiating events or the consequences of such events are limited because of good engineering design (e.g. multiple levels of redundancy). However, by not considering them directly, the importance to safety of these systems is not always apparent.

ONR requires comprehensive design basis analyses of all initiating events (meeting the requirements of SAP FA.5) occurring in UK ABWR systems such as (but not limited to):

- heating, ventilation and air conditioning (HVAC) systems
- cooling chain systems (i.e. the RCW, RSW and SW systems)
- compressed gas systems.

Partial failure of a system (e.g. failure of a single component or train) and total failure of a system due to a common cause failure (CCF) should be considered. Frequencies for such failures will need to be derived so that the appropriate deterministic rules can be applied (e.g. single failure criterion, diverse protection for frequent faults, worst permissible maintenance state etc). If the appropriate deterministic rules cannot be met, modifications should be considered and the design demonstrated to be ALARP. This may be in the form of additional systems or by improving the safety classification of aspects of the design.

Failures in all modes of reactor operation need to be considered. The consequences of failures on the fuel route, including the spent fuel pool, also need to be considered.

It is ONR's expectation that CCFs in safety Class 2 and Class 3 essential services or support systems are considered to be frequent events in design basis analyses. As a result of the more onerous engineering design requirements and standards applied, ONR expects that a CCF within a Class 1 system to be an infrequent event.

Additional transient analysis/deterministic safety analysis may be necessary to demonstrate that the relevant acceptance criteria are met. However, this will need to be preceded by detailed functional analyses to identify which parts of the design or specific components could challenge the ability of the considered system to deliver its required function.

It is recognised that Hitachi-GE has ongoing work to develop and apply it approach to the categorisation and classifying of systems, structures and components (SSCs), as well as work on failure modes and effects analyses (FMEA). It is anticipated these can make a useful contribution towards addressing this Regulatory Observation.

Regulatory Observation Actions

RO-ABWR-0010.A1

Hitachi-GE is required to demonstrate that its design basis safety case considers failures in essential services and support systems.

To achieve this, it is anticipated Hitachi-GE will need to do the following:

- Perform a functional analysis of all support systems and services to identify failures which can compromise their ability to deliver the required functions. Partial and complete failures need to be considered.
- In accordance with the system's classification and FMEA, determine frequencies attributable to such failures and, if appropriate, undertake design basis analyses to demonstrate the robustness of the UK ABWR design. Consequential failures, single failures in the safety measures and the worst normally permitted maintenance states need to be considered in accordance with SAP FA.6.
- Undertake transient analysis as required to demonstrate that the appropriate design basis acceptance criteria are met.

If initiating events are bounded by existing entries in the fault schedule, this should be clearly identified. Any new events not covered elsewhere will need to be added to the fault schedule.

All modes of reactor operation need to be considered, as well as any implications for the UK ABWR fuel route (including the spent fuel pool).

The safety functions performed by the support systems need to be clearly categorised, and the safety classification of components within the systems justified. The safety functions performed by protective measures that respond to any failures also need to be appropriately categorised and a classification then applied to these measures.

Where the current design cannot meet the appropriate design basis acceptance criteria, design changes or modifications should be identified. An ALARP justification should be given for the final design solution.

A topic report (or similar document) describing the design basis safety case for these faults, including fully populated fault schedule entries and any supporting transient analysis shall be completed and fully integrated into the subsequent revision of the PCSR.

Resolution required by: To be determined by the Hitachi-GE Resolution Plan

REQUESTING PARTY TO COMPLETE

Actual Acknowledgement date:	
RP stated Resolution Plan agreement date:	